FIG.1

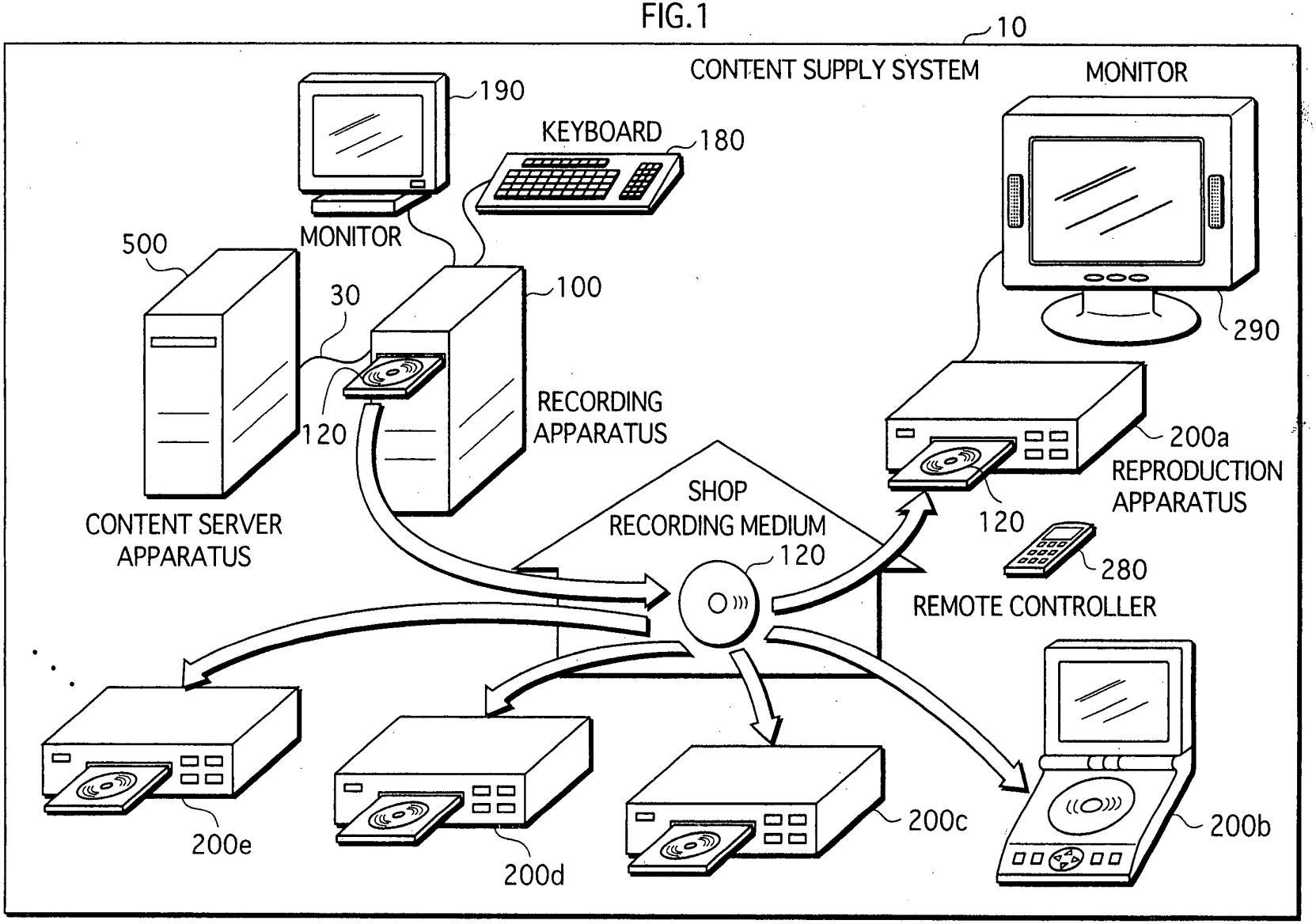

10
CONTENT SUPPLY SYSTEM
MONITOR
190
KEYBOARD
180
MONITOR
500
30
100
290
RECORDING
APPARATUS
120
200a
REPRODUCTION
APPARATUS
CONTENT SERVER
APPARATUS
SHOP
RECORDING MEDIUM
120
120
280
REMOTE CONTROLLER
200e
200d
200c
200b

FIG.2

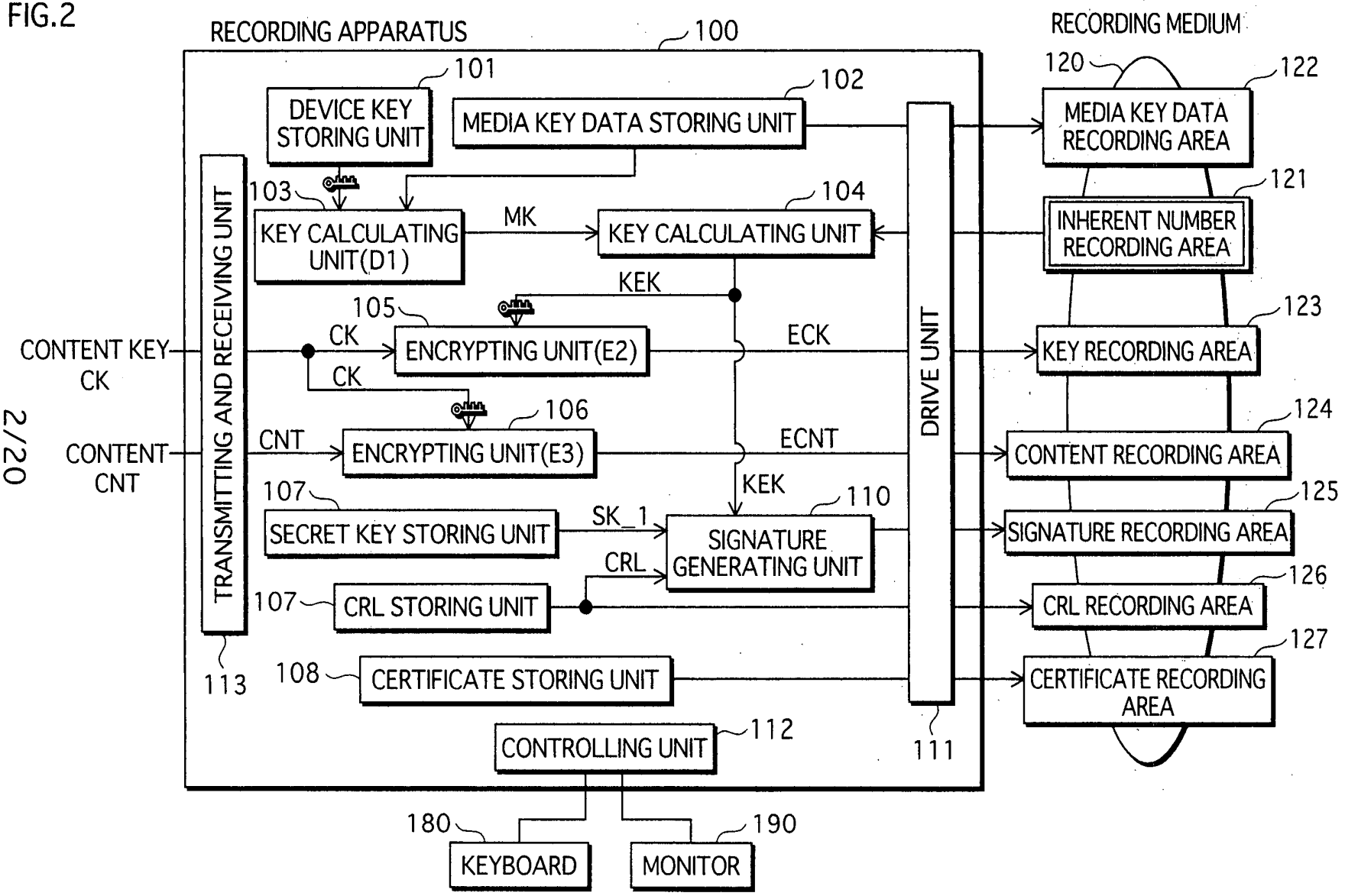

RECORDING APPARATUS
100
RECORDING MEDIUM
101
DEVICE KEY STORING UNIT
102
MEDIA KEY DATA STORING UNIT
120
122
MEDIA KEY DATA RECORDING AREA
103
KEY CALCULATING UNIT(D1)
MK
104
KEY CALCULATING UNIT
121
INHERENT NUMBER RECORDING AREA
KEK
105
CONTENT KEY
CK
CK
ENCRYPTING UNIT(E2)
ECK
123
KEY RECORDING AREA
CK
106
CONTENT
CNT
CNT
ENCRYPTING UNIT(E3)
ECNT
124
CONTENT RECORDING AREA
KEK
107
110
125
SECRET KEY STORING UNIT
SK_1
SIGNATURE GENERATING UNIT
SIGNATURE RECORDING AREA
CRL
126
107
CRL STORING UNIT
CRL RECORDING AREA
127
113
108
CERTIFICATE STORING UNIT
CERTIFICATE RECORDING AREA
112
CONTROLLING UNIT
111
180
190
KEYBOARD
MONITOR
TRANSMITTING AND RECEIVING UNIT
DRIVE UNIT

FIG.3

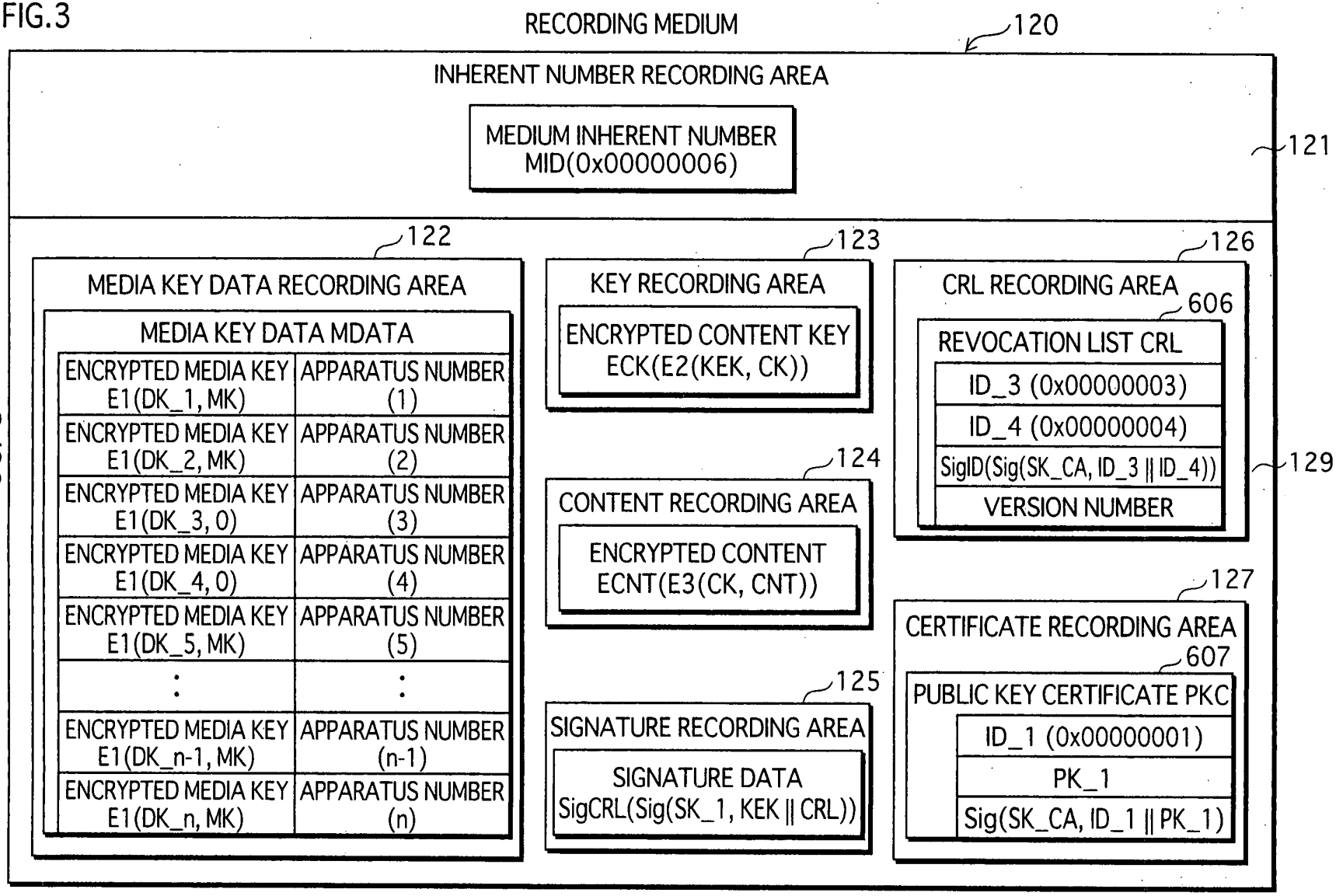

RECORDING MEDIUM
120
INHERENT NUMBER RECORDING AREA
MEDIUM INHERENT NUMBER
MID(0x00000006)
121
122
MEDIA KEY DATA RECORDING AREA
MEDIA KEY DATA MDATA
ENCRYPTED MEDIA KEY E1(DK_1, MK)
APPARATUS NUMBER (1)
ENCRYPTED MEDIA KEY E1(DK_2, MK)
APPARATUS NUMBER (2)
ENCRYPTED MEDIA KEY E1(DK_3, 0)
APPARATUS NUMBER (3)
ENCRYPTED MEDIA KEY E1(DK_4, 0)
APPARATUS NUMBER (4)
ENCRYPTED MEDIA KEY E1(DK_5, MK)
APPARATUS NUMBER (5)
ENCRYPTED MEDIA KEY E1(DK_n-1, MK)
APPARATUS NUMBER (n-1)
ENCRYPTED MEDIA KEY E1(DK_n, MK)
APPARATUS NUMBER (n)
123
KEY RECORDING AREA
ENCRYPTED CONTENT KEY ECK(E2(KEK, CK))
124
CONTENT RECORDING AREA
ENCRYPTED CONTENT ECNT(E3(CK, CNT))
125
SIGNATURE RECORDING AREA
SIGNATURE DATA SigCRL(Sig(SK_1, KEK || CRL))
126
CRL RECORDING AREA
606
REVOCATION LIST CRL
ID_3 (0x00000003)
ID_4 (0x00000004)
SigID(Sig(SK_CA, ID_3 || ID_4))
VERSION NUMBER
129
127
CERTIFICATE RECORDING AREA
607
PUBLIC KEY CERTIFICATE PKC
ID_1 (0x00000001)
PK_1
Sig(SK_CA, ID_1 || PK_1)

FIG.4

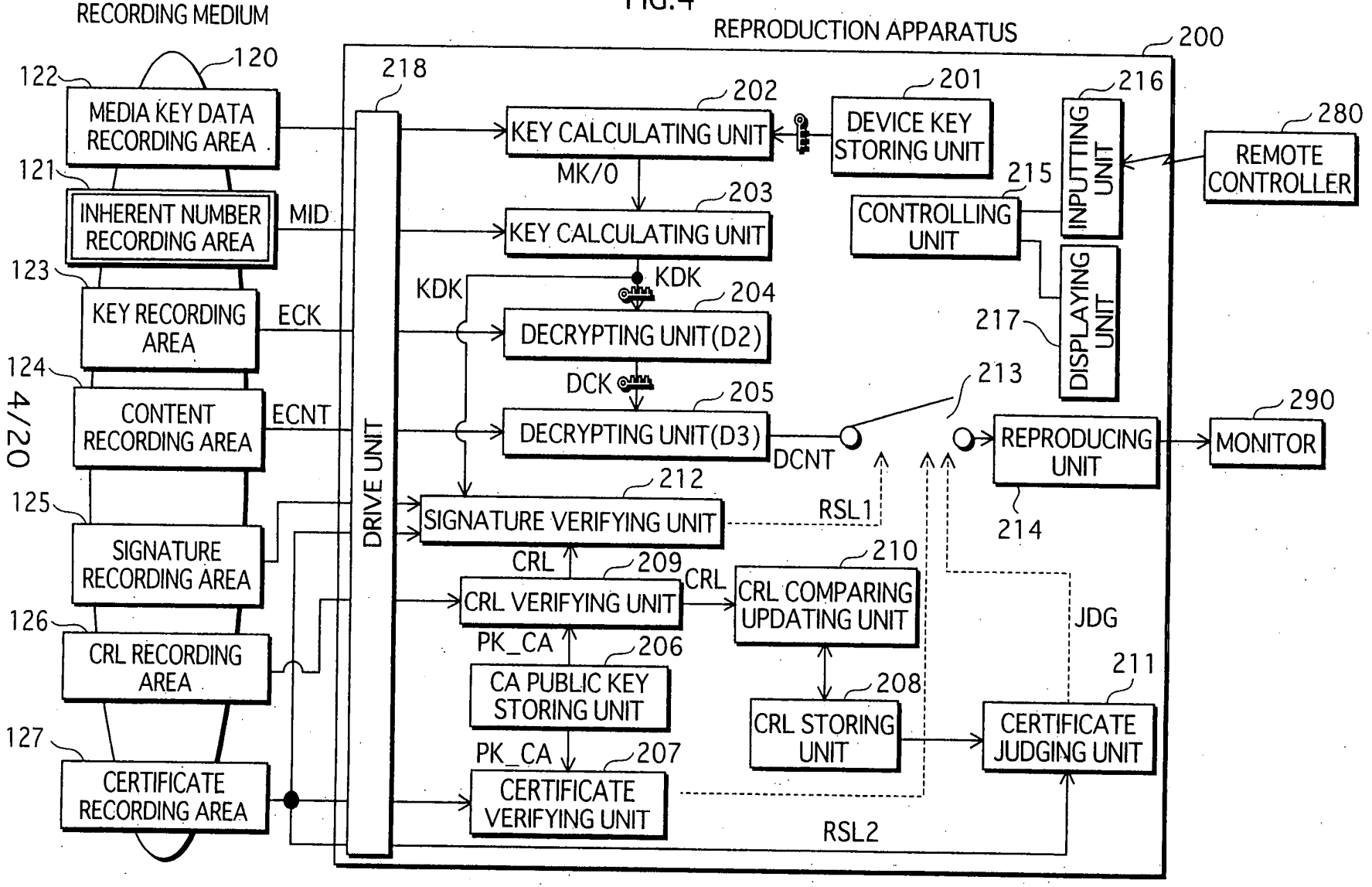

RECORDING MEDIUM
REPRODUCTION APPARATUS
200
120
122
MEDIA KEY DATA RECORDING AREA
121
INHERENT NUMBER RECORDING AREA
MID
123
KEY RECORDING AREA
ECK
124
CONTENT RECORDING AREA
ECNT
125
SIGNATURE RECORDING AREA
126
CRL RECORDING AREA
127
CERTIFICATE RECORDING AREA
218
DRIVE UNIT
202
KEY CALCULATING UNIT
MK/0
203
KEY CALCULATING UNIT
KDK
KDK
204
DECRYPTING UNIT(D2)
DCK
205
DECRYPTING UNIT(D3)
DCNT
212
SIGNATURE VERIFYING UNIT
RSL1
CRL
209
CRL VERIFYING UNIT
CRL
PK_CA
206
CA PUBLIC KEY STORING UNIT
PK_CA
207
CERTIFICATE VERIFYING UNIT
RSL2
201
DEVICE KEY STORING UNIT
215
CONTROLLING UNIT
216
INPUTTING UNIT
280
REMOTE CONTROLLER
217
DISPLAYING UNIT
213
214
REPRODUCING UNIT
290
MONITOR
210
CRL COMPARING UPDATING UNIT
JDG
208
CRL STORING UNIT
211
CERTIFICATE JUDGING UNIT

FIG.5

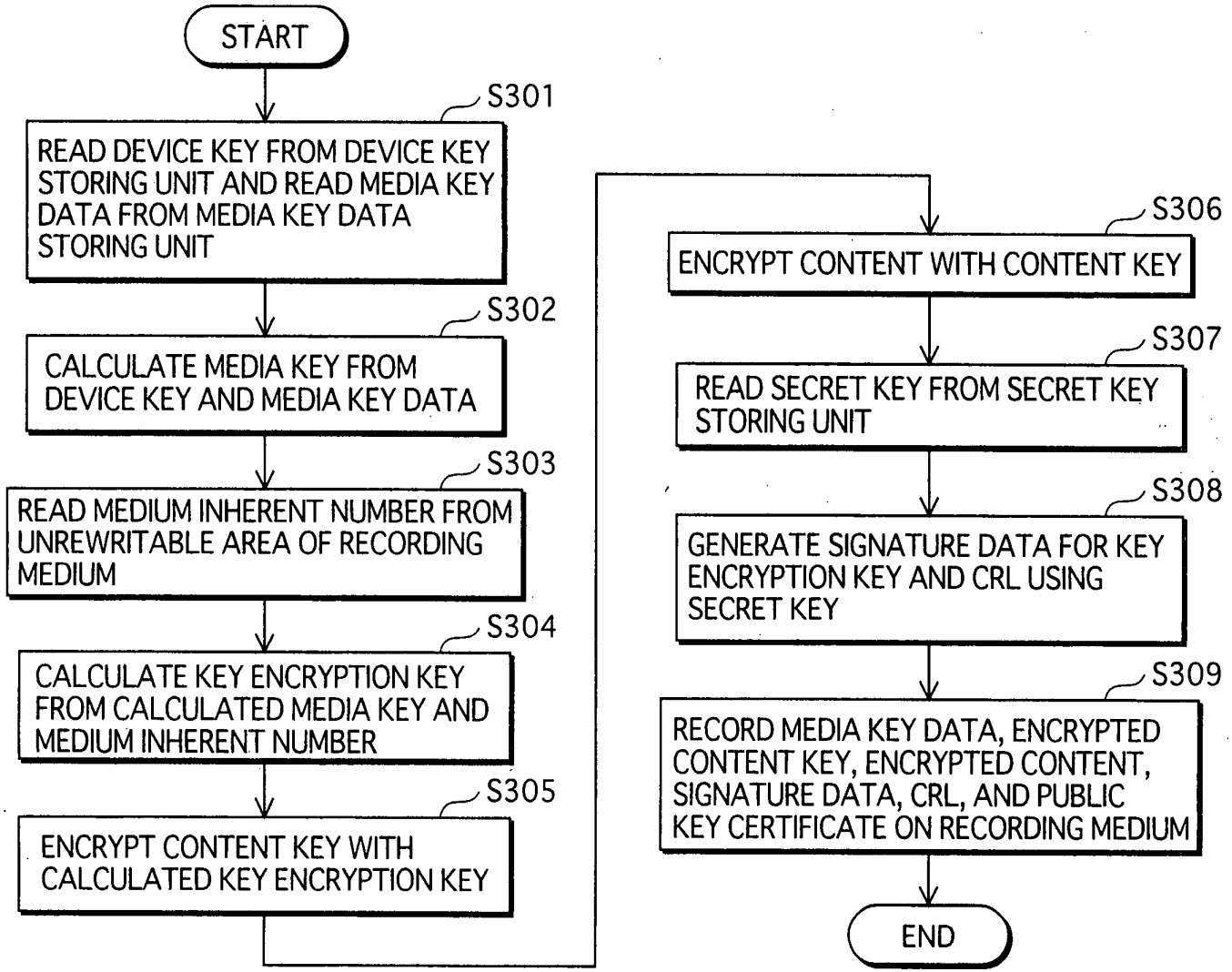

START
S301
READ DEVICE KEY FROM DEVICE KEY STORING UNIT AND READ MEDIA KEY DATA FROM MEDIA KEY DATA STORING UNIT
S302
CALCULATE MEDIA KEY FROM DEVICE KEY AND MEDIA KEY DATA
S303
READ MEDIUM INHERENT NUMBER FROM UNREWRITABLE AREA OF RECORDING MEDIUM
S304
CALCULATE KEY ENCRYPTION KEY FROM CALCULATED MEDIA KEY AND MEDIUM INHERENT NUMBER
S305
ENCRYPT CONTENT KEY WITH CALCULATED KEY ENCRYPTION KEY
S306
ENCRYPT CONTENT WITH CONTENT KEY
S307
READ SECRET KEY FROM SECRET KEY STORING UNIT
S308
GENERATE SIGNATURE DATA FOR KEY ENCRYPTION KEY AND CRL USING SECRET KEY
S309
RECORD MEDIA KEY DATA, ENCRYPTED CONTENT KEY, ENCRYPTED CONTENT, SIGNATURE DATA, CRL, AND PUBLIC KEY CERTIFICATE ON RECORDING MEDIUM
END

FIG.6

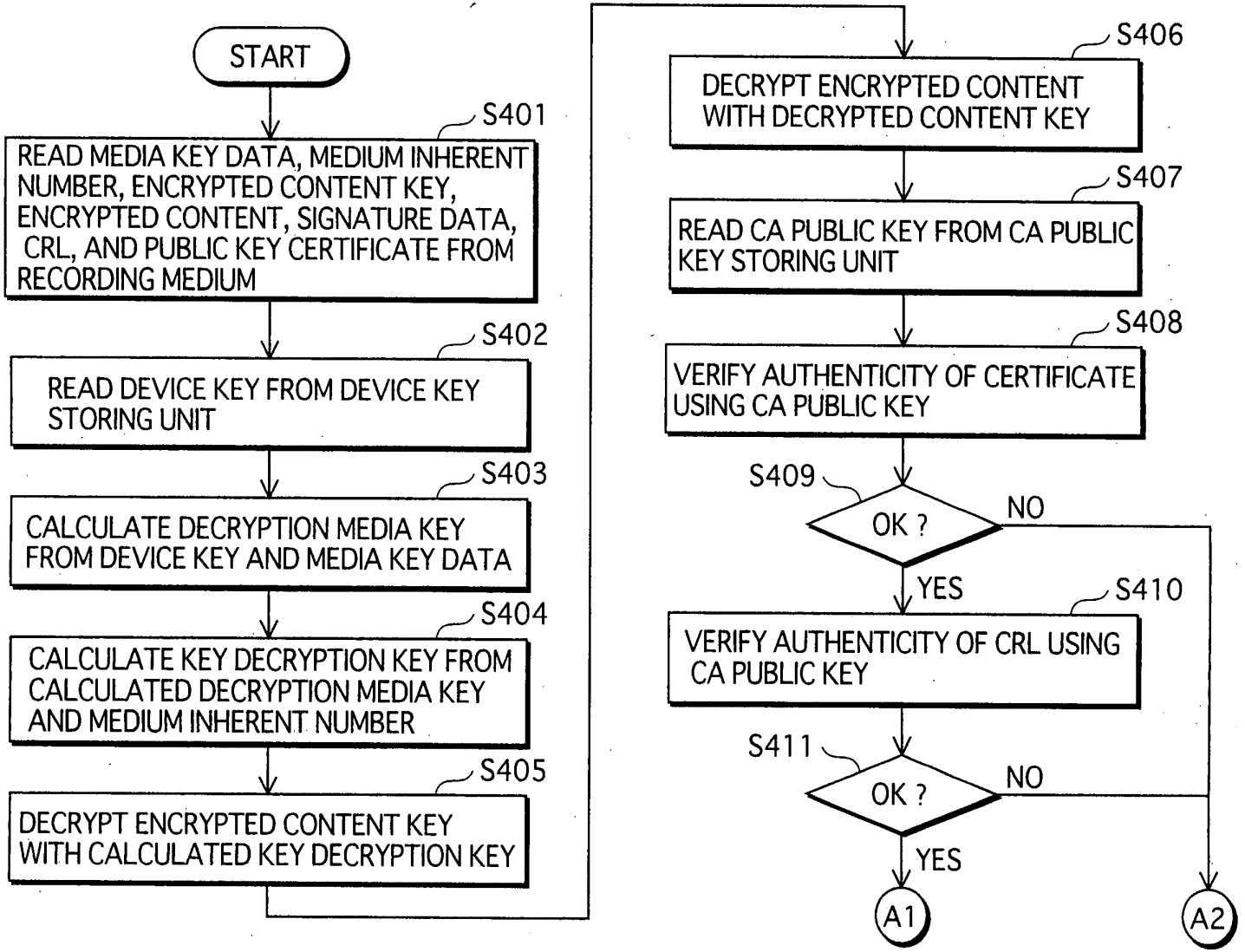

START
S401
READ MEDIA KEY DATA, MEDIUM INHERENT NUMBER, ENCRYPTED CONTENT KEY, ENCRYPTED CONTENT, SIGNATURE DATA, CRL, AND PUBLIC KEY CERTIFICATE FROM RECORDING MEDIUM
S402
READ DEVICE KEY FROM DEVICE KEY STORING UNIT
S403
CALCULATE DECRYPTION MEDIA KEY FROM DEVICE KEY AND MEDIA KEY DATA
S404
CALCULATE KEY DECRYPTION KEY FROM CALCULATED DECRYPTION MEDIA KEY AND MEDIUM INHERENT NUMBER
S405
DECRYPT ENCRYPTED CONTENT KEY WITH CALCULATED KEY DECRYPTION KEY
S406
DECRYPT ENCRYPTED CONTENT WITH DECRYPTED CONTENT KEY
S407
READ CA PUBLIC KEY FROM CA PUBLIC KEY STORING UNIT
S408
VERIFY AUTHENTICITY OF CERTIFICATE USING CA PUBLIC KEY
S409
OK ?
NO
YES
S410
VERIFY AUTHENTICITY OF CRL USING CA PUBLIC KEY
S411
OK ?
NO
YES
A1
A2

FIG.7

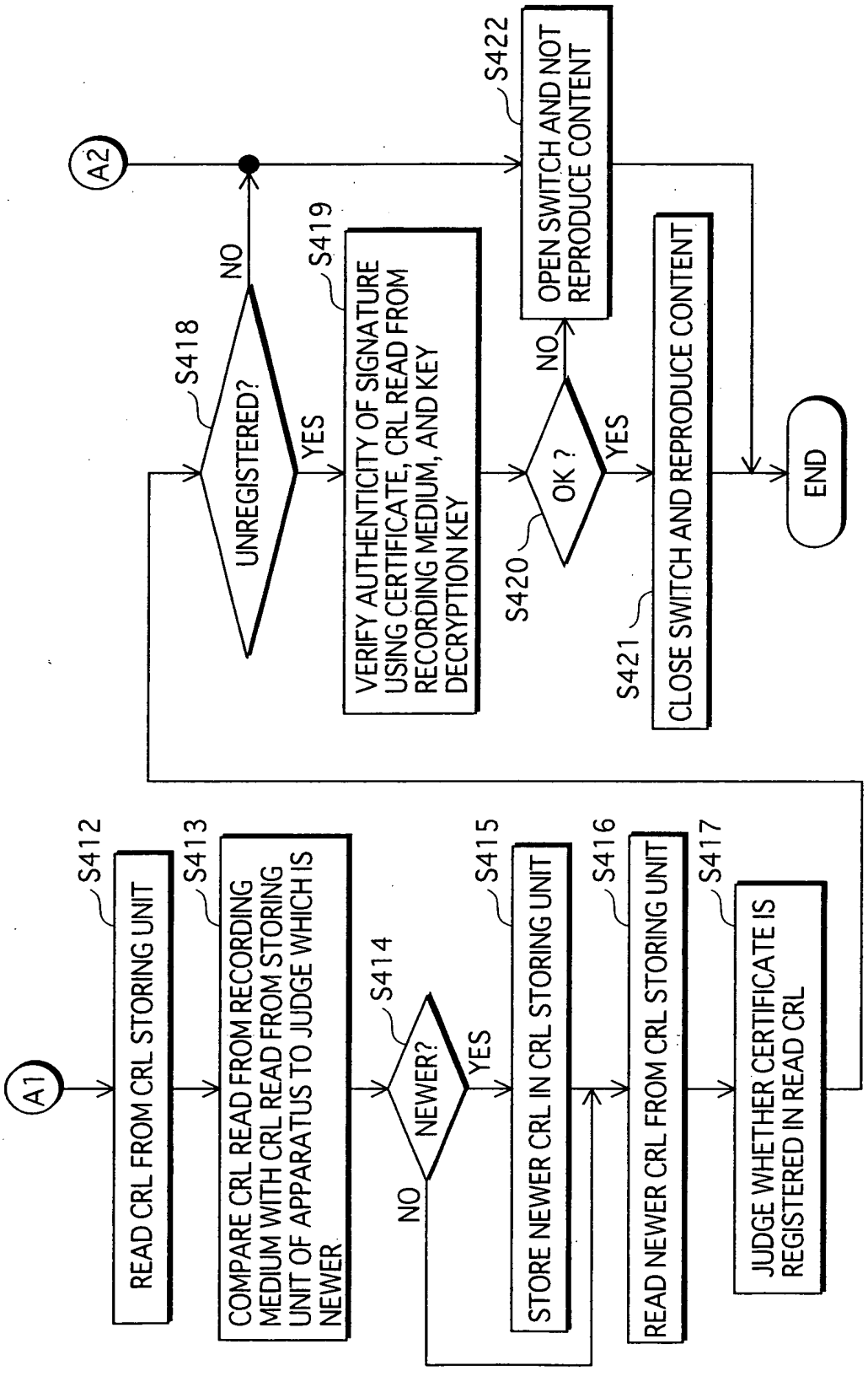

A1
S412
READ CRL FROM CRL STORING UNIT
S413
COMPARE CRL READ FROM RECORDING MEDIUM WITH CRL READ FROM STORING UNIT OF APPARATUS TO JUDGE WHICH IS NEWER
S414
NEWER?
YES
NO
S415
STORE NEWER CRL IN CRL STORING UNIT
S416
READ NEWER CRL FROM CRL STORING UNIT
S417
JUDGE WHETHER CERTIFICATE IS REGISTERED IN READ CRL
A2
S418
UNREGISTERED?
YES
NO
S419
VERIFY AUTHENTICITY OF SIGNATURE USING CERTIFICATE, CRL READ FROM RECORDING MEDIUM, AND KEY DECRYPTION KEY
S420
OK ?
YES
NO
S421
CLOSE SWITCH AND REPRODUCE CONTENT
S422
OPEN SWITCH AND NOT REPRODUCE CONTENT
END

FIG.8

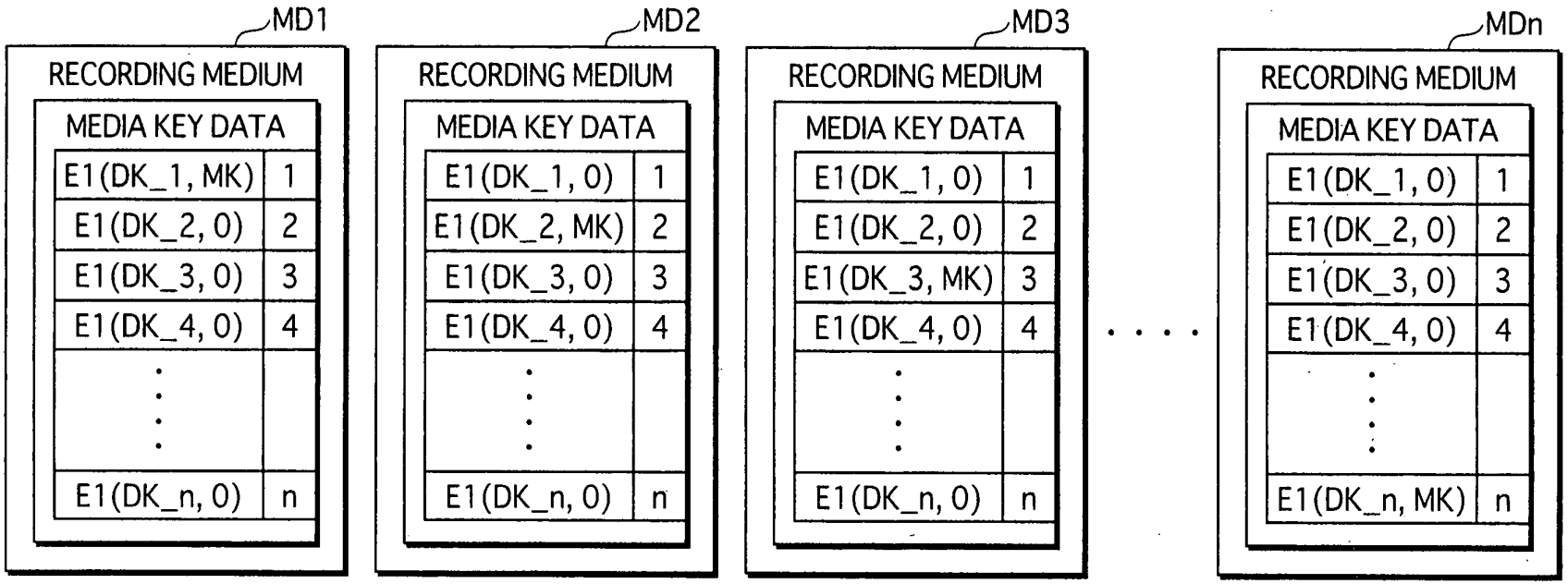

MD1
RECORDING MEDIUM
MEDIA KEY DATA
E1(DK_1, MK) 1
E1(DK_2, 0) 2
E1(DK_3, 0) 3
E1(DK_4, 0) 4
E1(DK_n, 0) n
MD2
RECORDING MEDIUM
MEDIA KEY DATA
E1(DK_1, 0) 1
E1(DK_2, MK) 2
E1(DK_3, 0) 3
E1(DK_4, 0) 4
E1(DK_n, 0) n
MD3
RECORDING MEDIUM
MEDIA KEY DATA
E1(DK_1, 0) 1
E1(DK_2, 0) 2
E1(DK_3, MK) 3
E1(DK_4, 0) 4
E1(DK_n, 0) n
MDn
RECORDING MEDIUM
MEDIA KEY DATA
E1(DK_1, 0) 1
E1(DK_2, 0) 2
E1(DK_3, 0) 3
E1(DK_4, 0) 4
E1(DK_n, MK) n

FIG.9

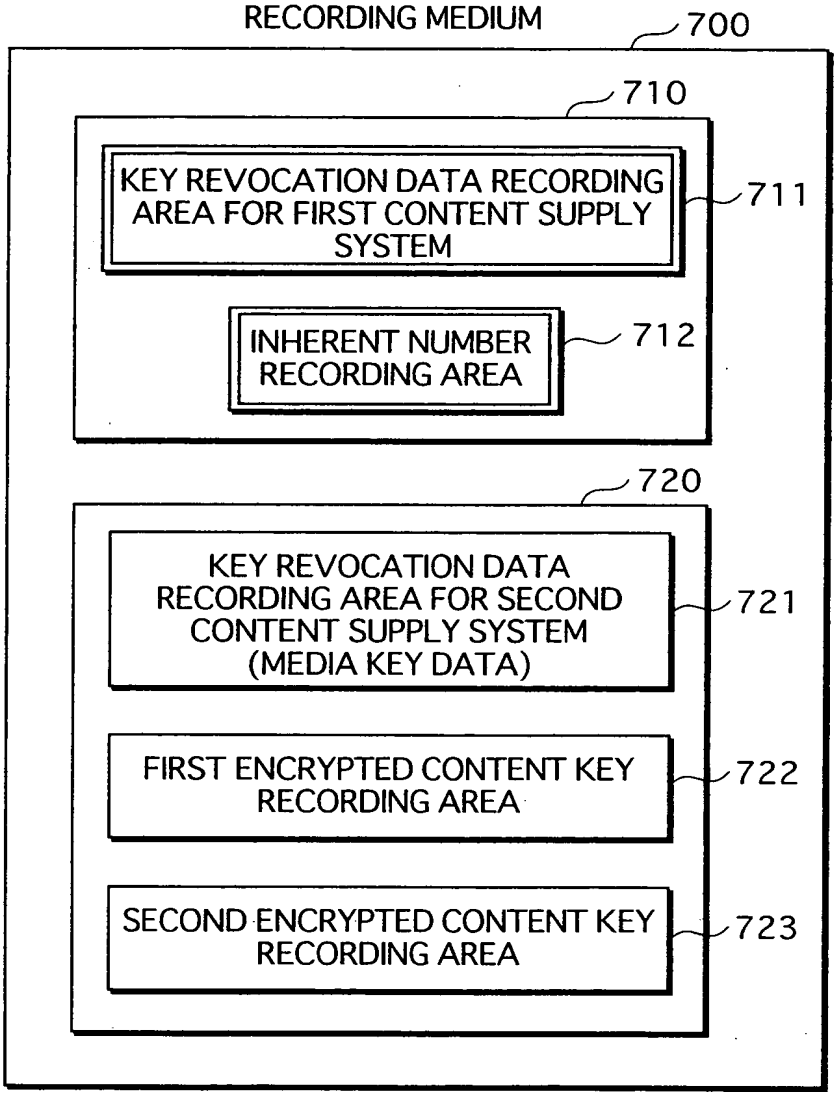

RECORDING MEDIUM
700
710
KEY REVOCATION DATA RECORDING AREA FOR FIRST CONTENT SUPPLY SYSTEM
711
INHERENT NUMBER RECORDING AREA
712
720
KEY REVOCATION DATA RECORDING AREA FOR SECOND CONTENT SUPPLY SYSTEM (MEDIA KEY DATA)
721
FIRST ENCRYPTED CONTENT KEY RECORDING AREA
722
SECOND ENCRYPTED CONTENT KEY RECORDING AREA
723

FIG.10

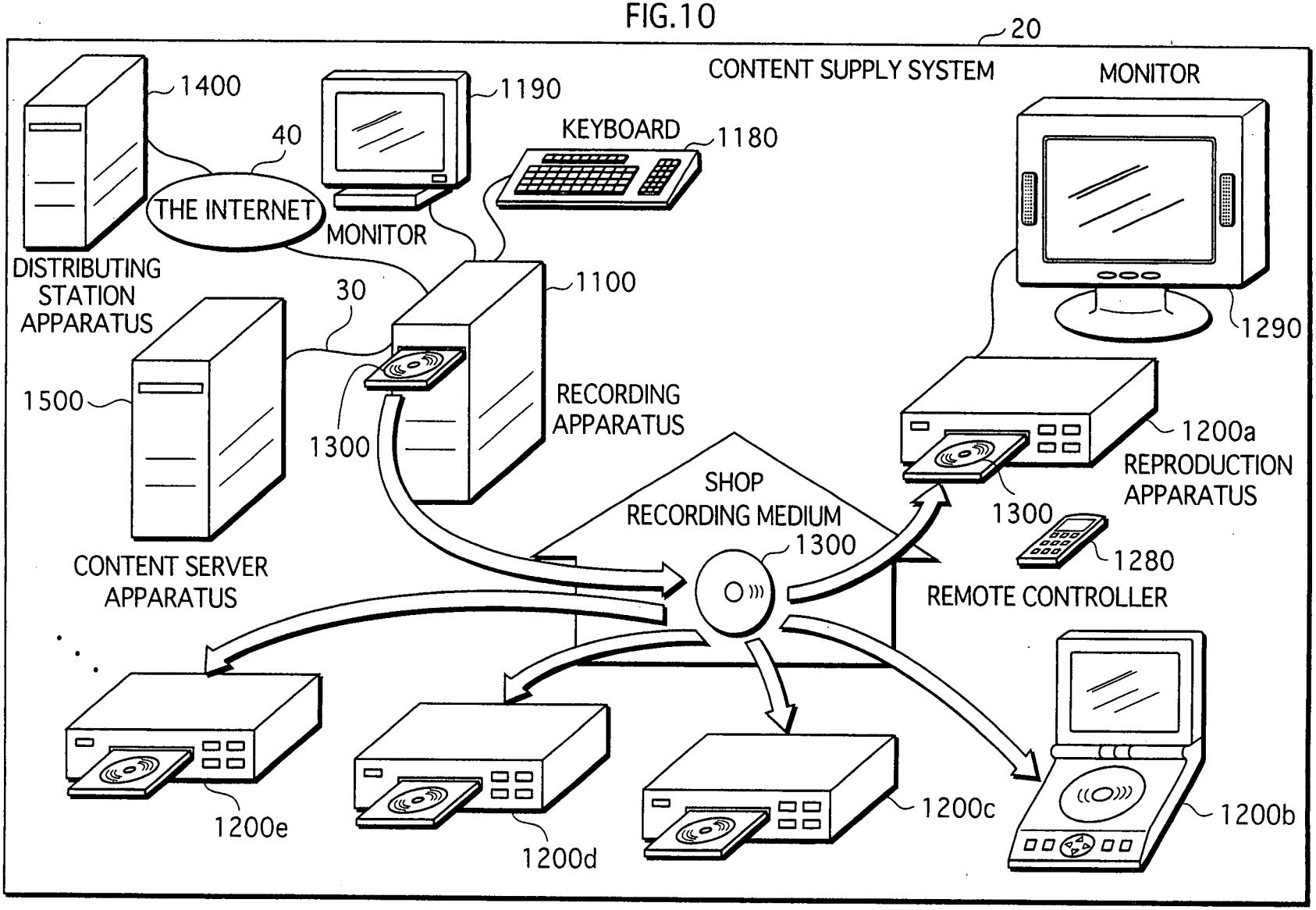

20
CONTENT SUPPLY SYSTEM
MONITOR
1400
1190
KEYBOARD
1180
40
THE INTERNET
MONITOR
DISTRIBUTING STATION APPARATUS
30
1100
1290
1500
RECORDING APPARATUS
1300
1200a
REPRODUCTION APPARATUS
SHOP RECORDING MEDIUM
1300
1300
1280
REMOTE CONTROLLER
CONTENT SERVER APPARATUS
1200e
1200d
1200c
1200b

FIG.11

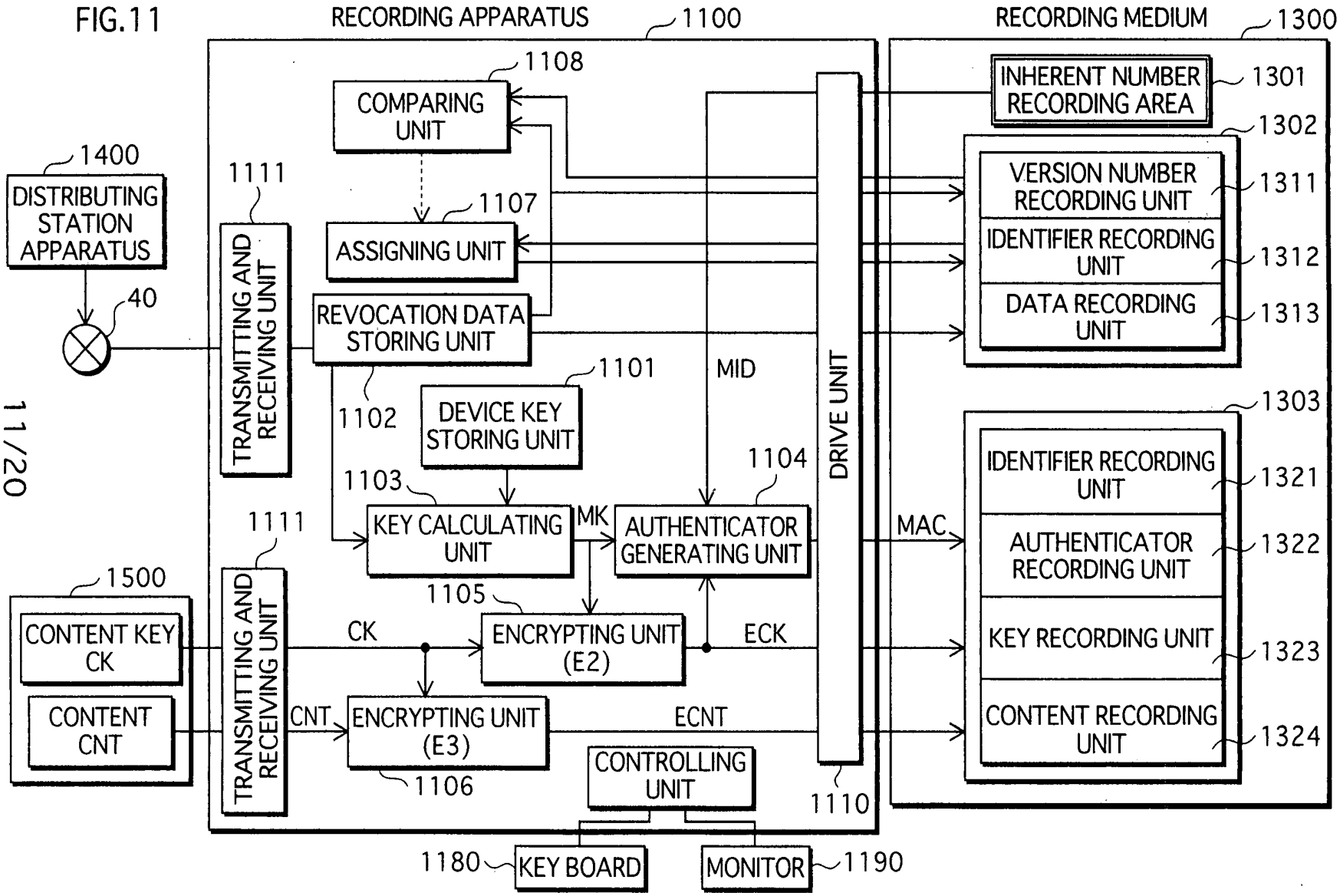

RECORDING APPARATUS
1100
RECORDING MEDIUM
1300
1108
COMPARING UNIT
INHERENT NUMBER RECORDING AREA
1301
1302
1400
DISTRIBUTING STATION APPARATUS
1111
1107
ASSIGNING UNIT
VERSION NUMBER RECORDING UNIT
1311
IDENTIFIER RECORDING UNIT
1312
DATA RECORDING UNIT
1313
40
TRANSMITTING AND RECEIVING UNIT
REVOCATION DATA STORING UNIT
1101
MID
1102
DEVICE KEY STORING UNIT
1303
1104
1103
IDENTIFIER RECORDING UNIT
1321
KEY CALCULATING UNIT
MK
AUTHENTICATOR GENERATING UNIT
DRIVE UNIT
MAC
AUTHENTICATOR RECORDING UNIT
1322
1111
1500
1105
CONTENT KEY CK
CK
ENCRYPTING UNIT (E2)
ECK
KEY RECORDING UNIT
1323
CONTENT CNT
CNT
ENCRYPTING UNIT (E3)
ECNT
CONTENT RECORDING UNIT
1324
1106
CONTROLLING UNIT
1110
1180
KEY BOARD
MONITOR
1190

FIG.12

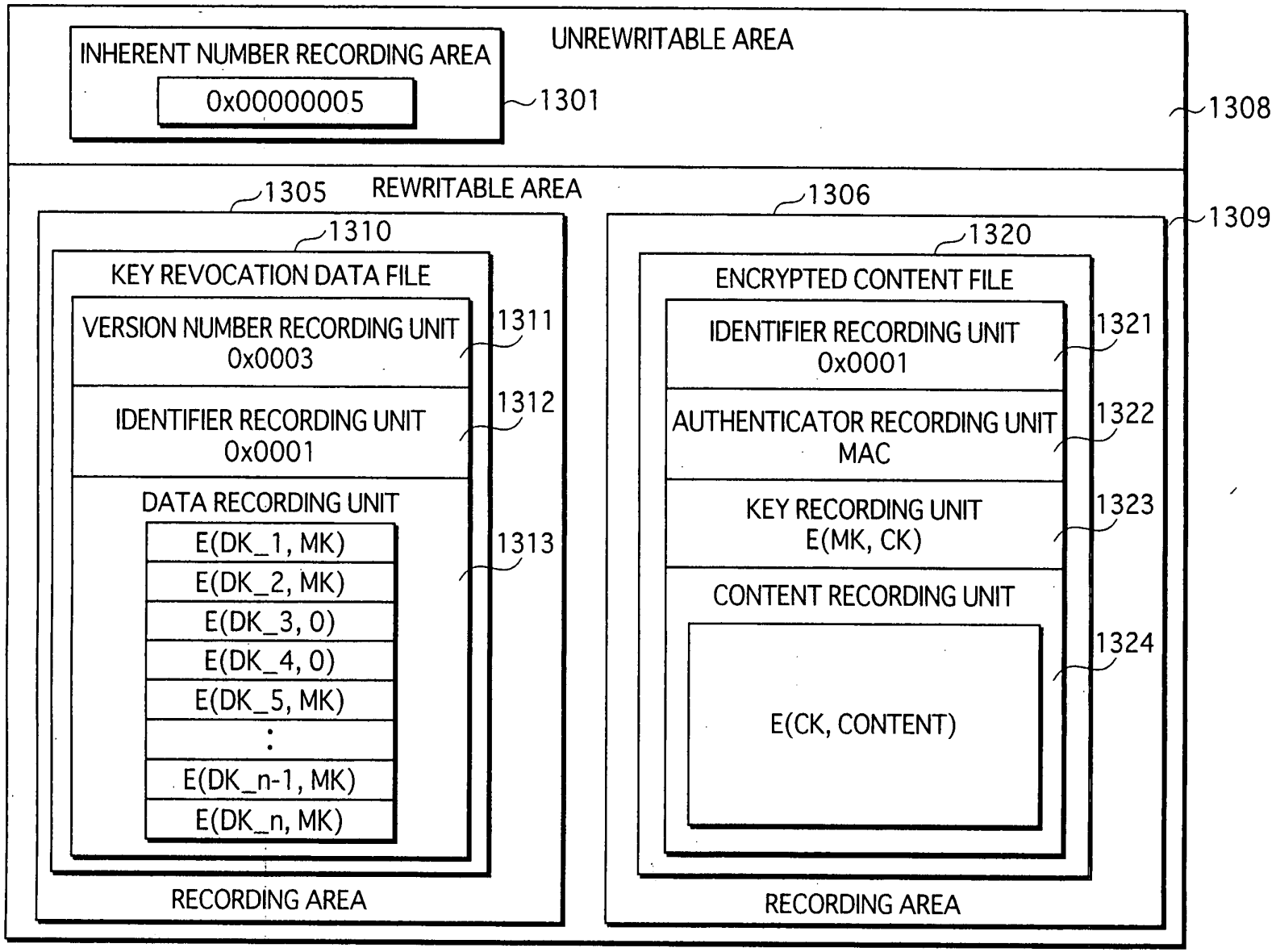

INHERENT NUMBER RECORDING AREA
0x00000005
1301
UNREWRITABLE AREA
1308
1305
REWRITABLE AREA
1306
1309
1310
KEY REVOCATION DATA FILE
VERSION NUMBER RECORDING UNIT
0x0003
1311
IDENTIFIER RECORDING UNIT
0x0001
1312
DATA RECORDING UNIT
E(DK_1, MK)
E(DK_2, MK)
E(DK_3, 0)
E(DK_4, 0)
E(DK_5, MK)
E(DK_n-1, MK)
E(DK_n, MK)
1313
RECORDING AREA
1320
ENCRYPTED CONTENT FILE
IDENTIFIER RECORDING UNIT
0x0001
1321
AUTHENTICATOR RECORDING UNIT
MAC
1322
KEY RECORDING UNIT
E(MK, CK)
1323
CONTENT RECORDING UNIT
E(CK, CONTENT)
1324
RECORDING AREA

FIG.13

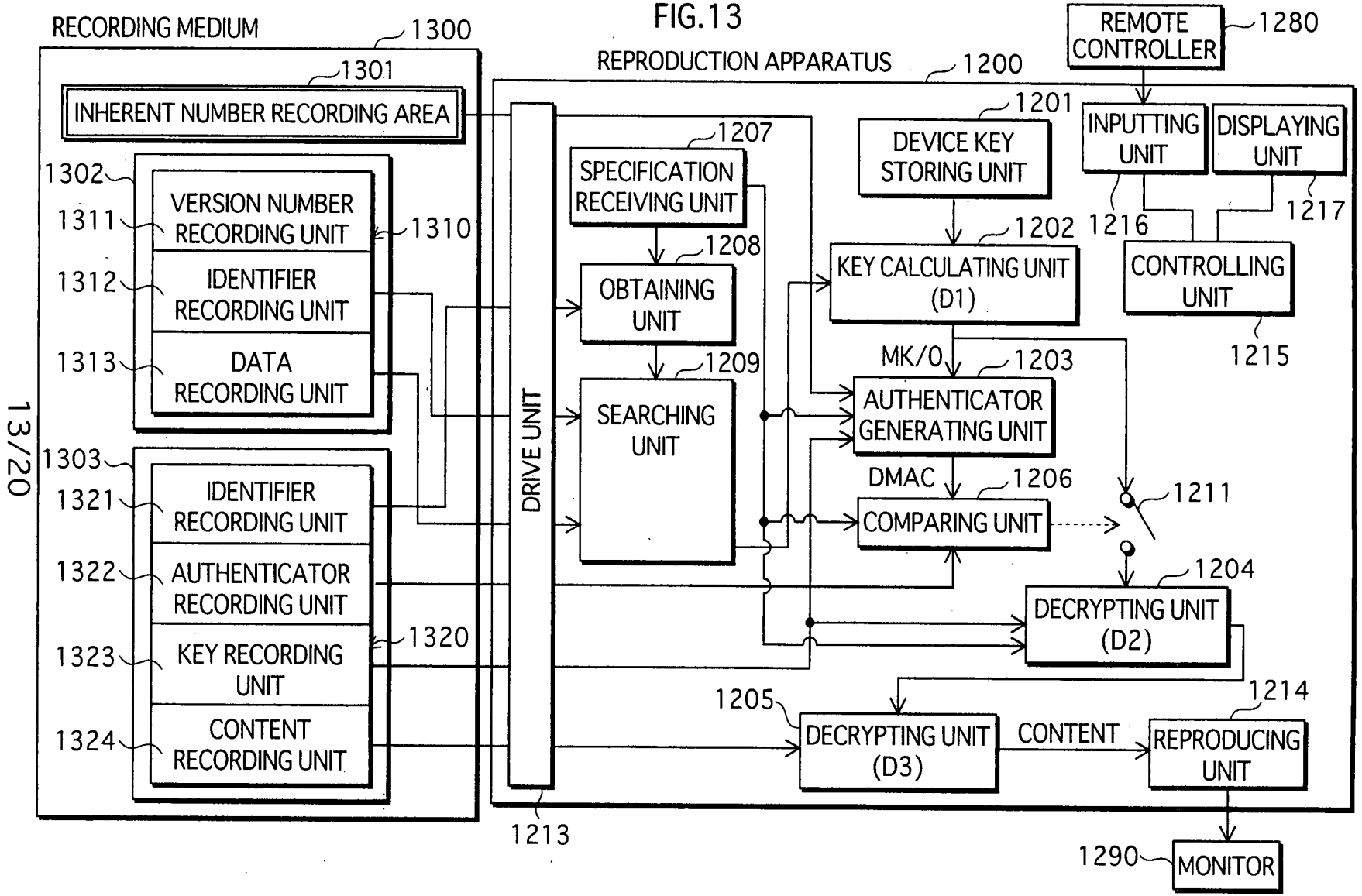

RECORDING MEDIUM
1300
1301
INHERENT NUMBER RECORDING AREA
1302
1311
VERSION NUMBER RECORDING UNIT
1310
1312
IDENTIFIER RECORDING UNIT
1313
DATA RECORDING UNIT
1303
1321
IDENTIFIER RECORDING UNIT
1322
AUTHENTICATOR RECORDING UNIT
1320
1323
KEY RECORDING UNIT
1324
CONTENT RECORDING UNIT
DRIVE UNIT
1213
REPRODUCTION APPARATUS
1200
REMOTE CONTROLLER
1280
1201
DEVICE KEY STORING UNIT
INPUTTING UNIT
DISPLAYING UNIT
1216
1217
1207
SPECIFICATION RECEIVING UNIT
1202
KEY CALCULATING UNIT (D1)
CONTROLLING UNIT
1215
1208
OBTAINING UNIT
MK/O
1203
AUTHENTICATOR GENERATING UNIT
1209
SEARCHING UNIT
DMAC
1206
1211
COMPARING UNIT
1204
DECRYPTING UNIT (D2)
1205
1214
DECRYPTING UNIT (D3)
CONTENT
REPRODUCING UNIT
1290
MONITOR

FIG.14

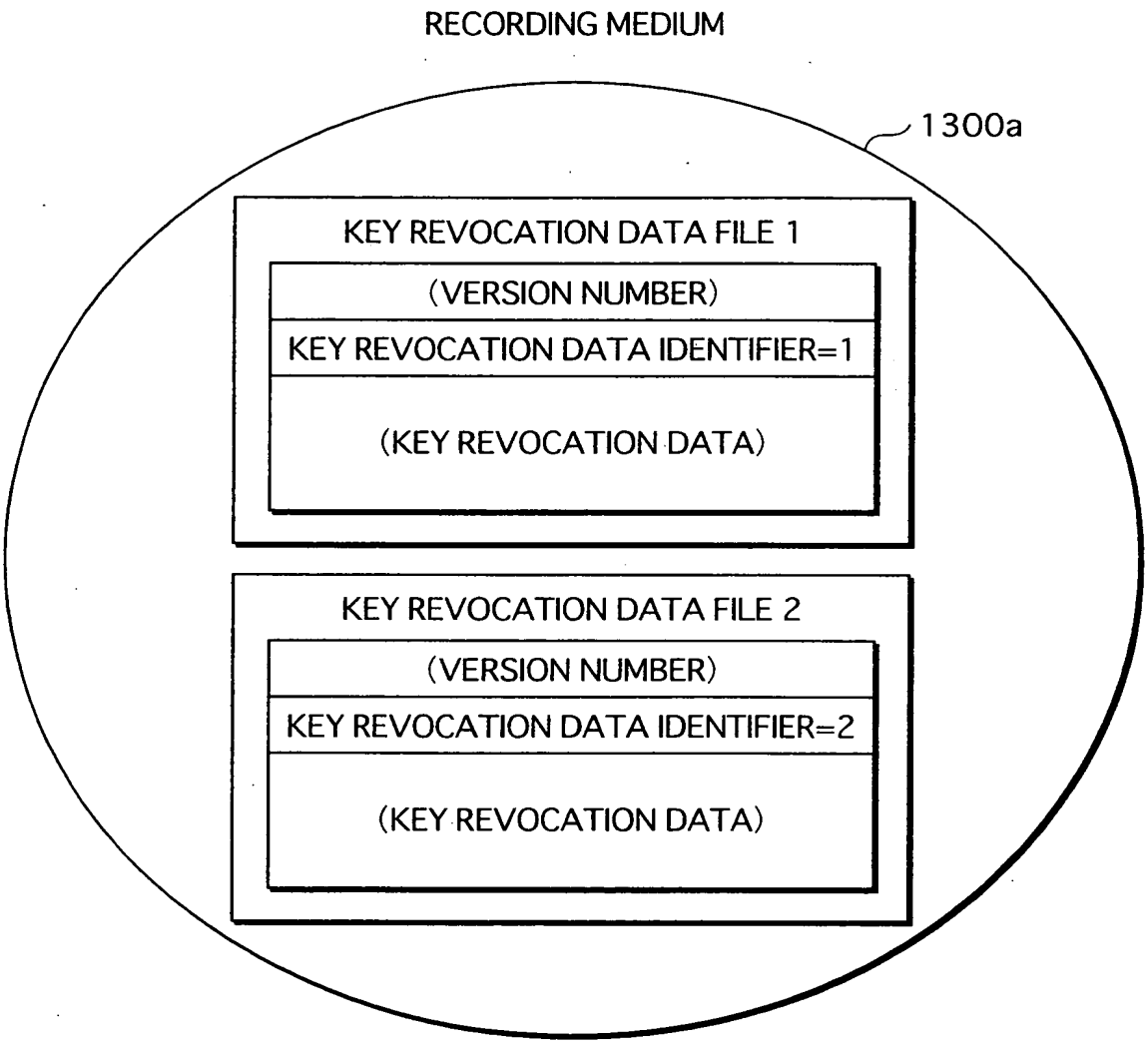

RECORDING MEDIUM
1300a
KEY REVOCATION DATA FILE 1
(VERSION NUMBER)
KEY REVOCATION DATA IDENTIFIER=1
(KEY REVOCATION DATA)
KEY REVOCATION DATA FILE 2
(VERSION NUMBER)
KEY REVOCATION DATA IDENTIFIER=2
(KEY REVOCATION DATA)

FIG.15

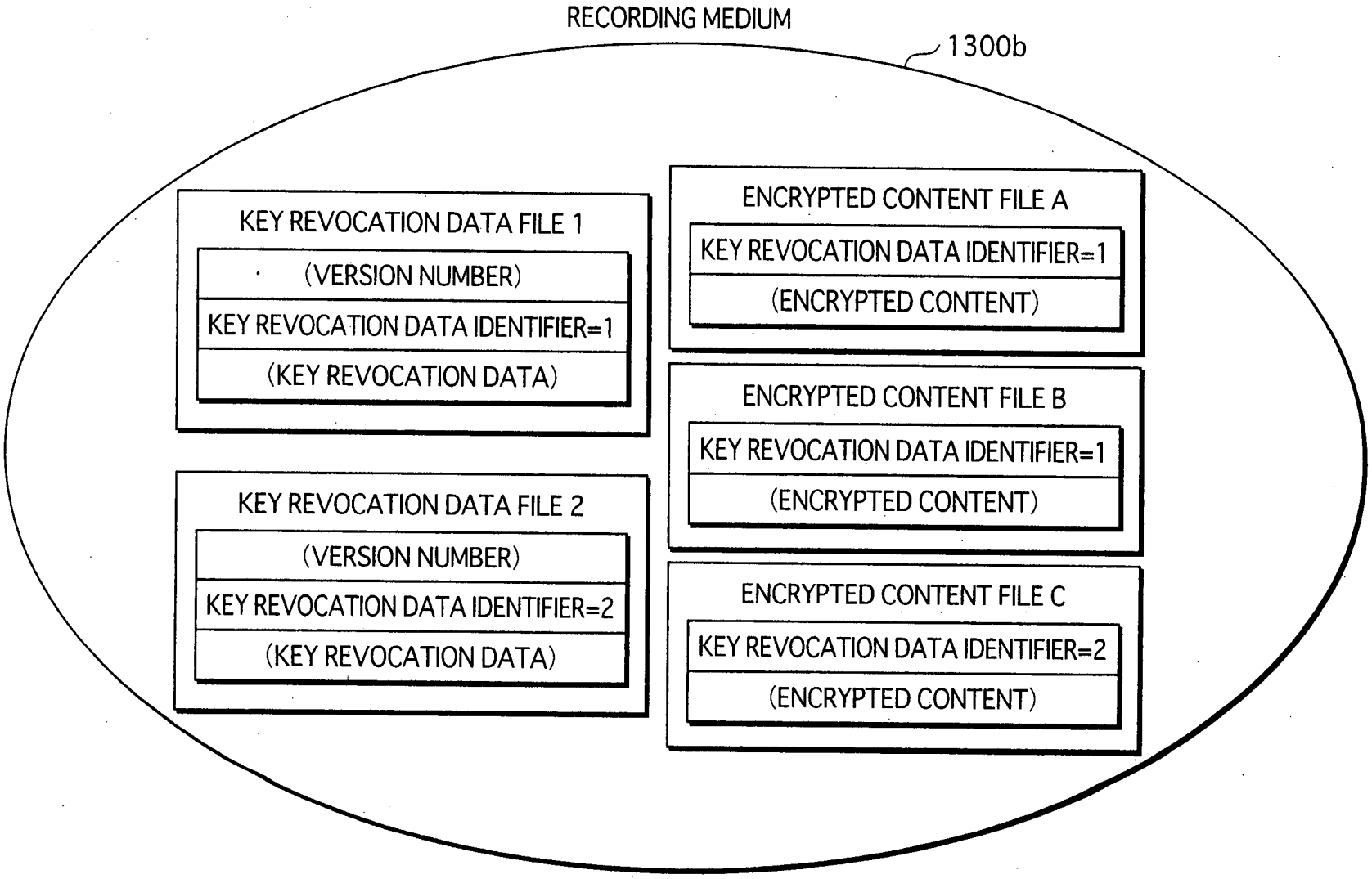

RECORDING MEDIUM
1300b
KEY REVOCATION DATA FILE 1
(VERSION NUMBER)
KEY REVOCATION DATA IDENTIFIER=1
(KEY REVOCATION DATA)
KEY REVOCATION DATA FILE 2
(VERSION NUMBER)
KEY REVOCATION DATA IDENTIFIER=2
(KEY REVOCATION DATA)
ENCRYPTED CONTENT FILE A
KEY REVOCATION DATA IDENTIFIER=1
(ENCRYPTED CONTENT)
ENCRYPTED CONTENT FILE B
KEY REVOCATION DATA IDENTIFIER=1
(ENCRYPTED CONTENT)
ENCRYPTED CONTENT FILE C
KEY REVOCATION DATA IDENTIFIER=2
(ENCRYPTED CONTENT)

FIG.16

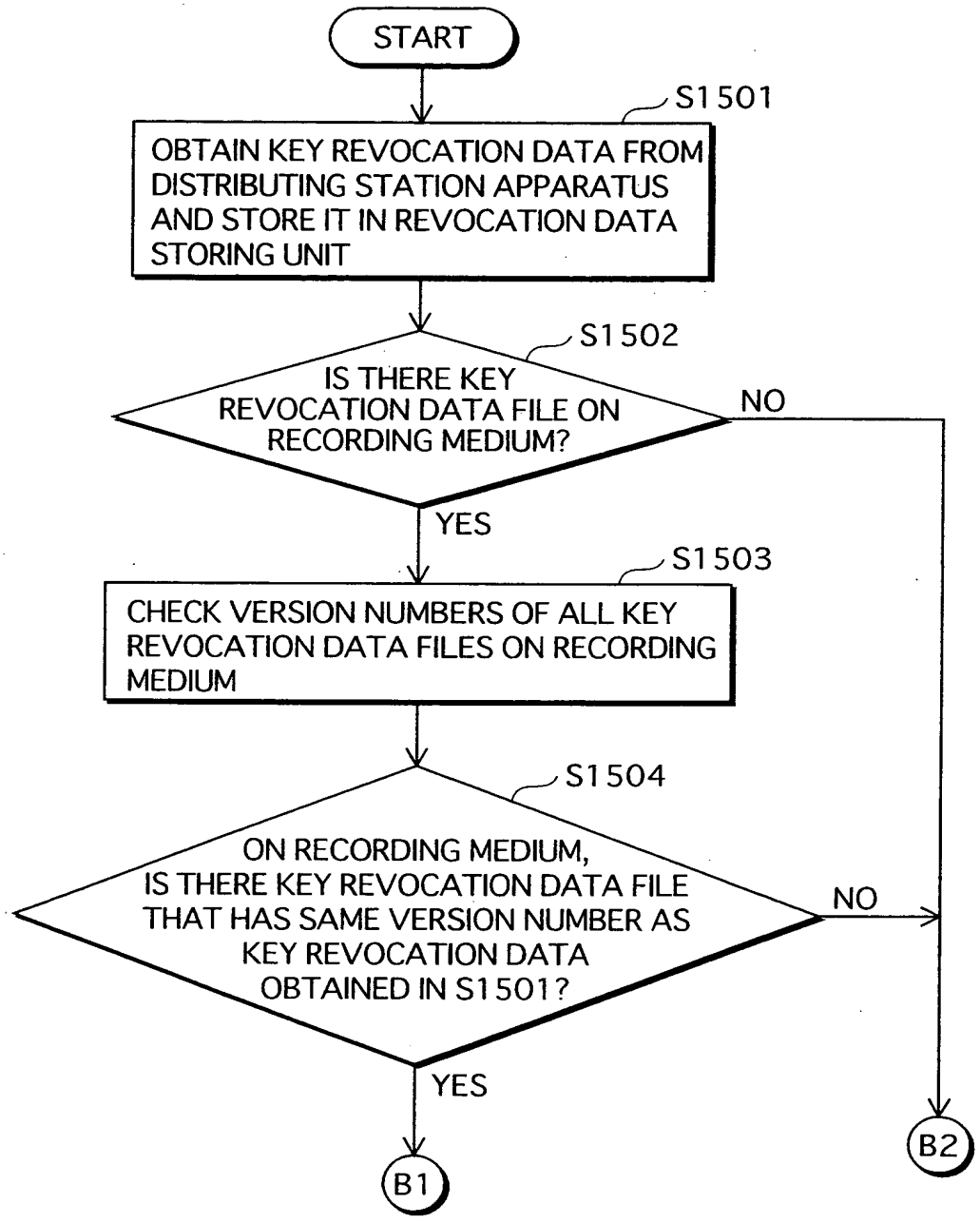

START
S1501
OBTAIN KEY REVOCATION DATA FROM DISTRIBUTING STATION APPARATUS AND STORE IT IN REVOCATION DATA STORING UNIT
S1502
IS THERE KEY REVOCATION DATA FILE ON RECORDING MEDIUM?
NO
YES
S1503
CHECK VERSION NUMBERS OF ALL KEY REVOCATION DATA FILES ON RECORDING MEDIUM
S1504
ON RECORDING MEDIUM, IS THERE KEY REVOCATION DATA FILE THAT HAS SAME VERSION NUMBER AS KEY REVOCATION DATA OBTAINED IN S1501?
NO
YES
B1
B2

FIG.17

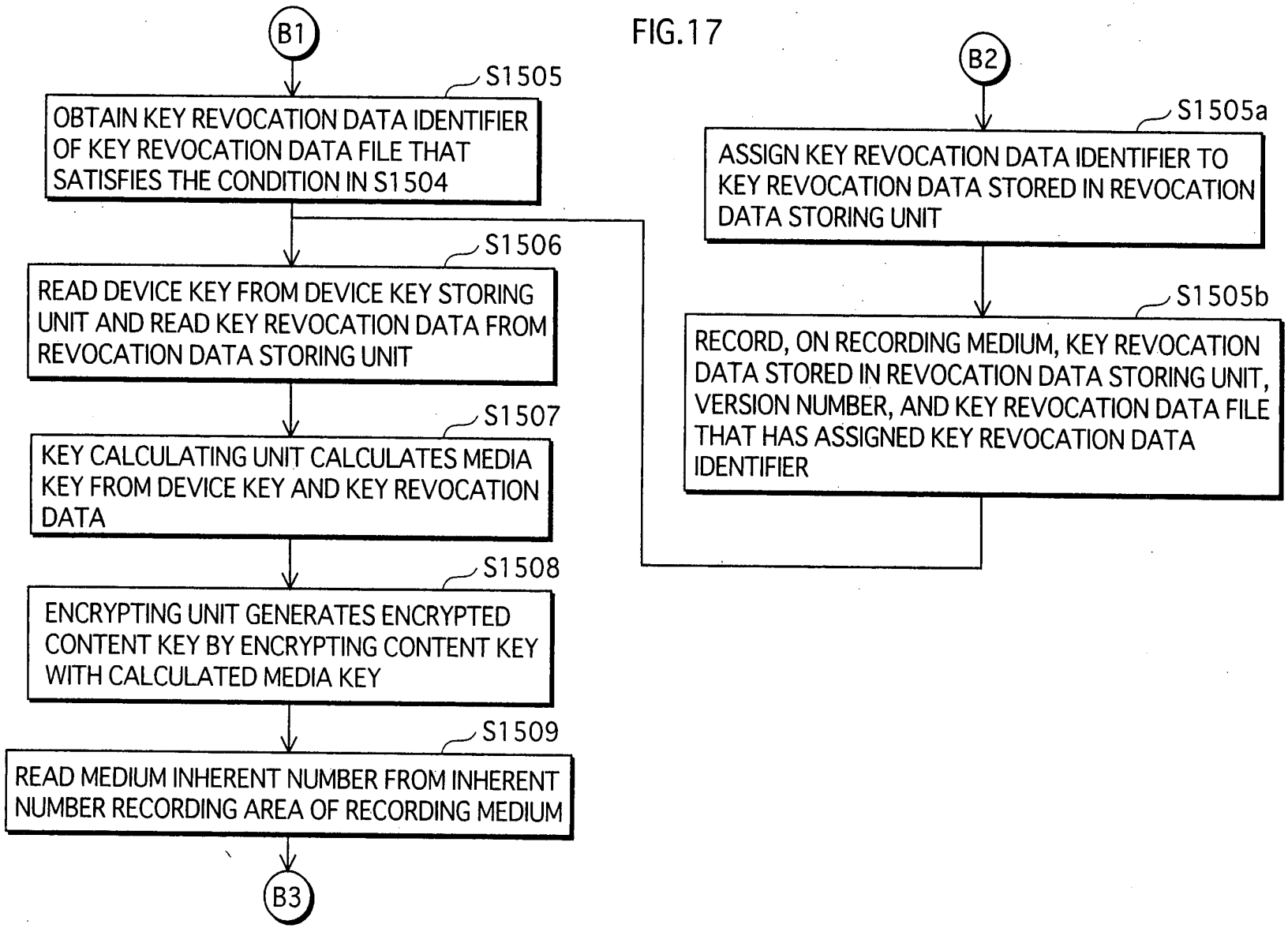

B1
S1505
OBTAIN KEY REVOCATION DATA IDENTIFIER OF KEY REVOCATION DATA FILE THAT SATISFIES THE CONDITION IN S1504
S1506
READ DEVICE KEY FROM DEVICE KEY STORING UNIT AND READ KEY REVOCATION DATA FROM REVOCATION DATA STORING UNIT
S1507
KEY CALCULATING UNIT CALCULATES MEDIA KEY FROM DEVICE KEY AND KEY REVOCATION DATA
S1508
ENCRYPTING UNIT GENERATES ENCRYPTED CONTENT KEY BY ENCRYPTING CONTENT KEY WITH CALCULATED MEDIA KEY
S1509
READ MEDIUM INHERENT NUMBER FROM INHERENT NUMBER RECORDING AREA OF RECORDING MEDIUM
B3
B2
S1505a
ASSIGN KEY REVOCATION DATA IDENTIFIER TO KEY REVOCATION DATA STORED IN REVOCATION DATA STORING UNIT
S1505b
RECORD, ON RECORDING MEDIUM, KEY REVOCATION DATA STORED IN REVOCATION DATA STORING UNIT, VERSION NUMBER, AND KEY REVOCATION DATA FILE THAT HAS ASSIGNED KEY REVOCATION DATA IDENTIFIER

FIG.18

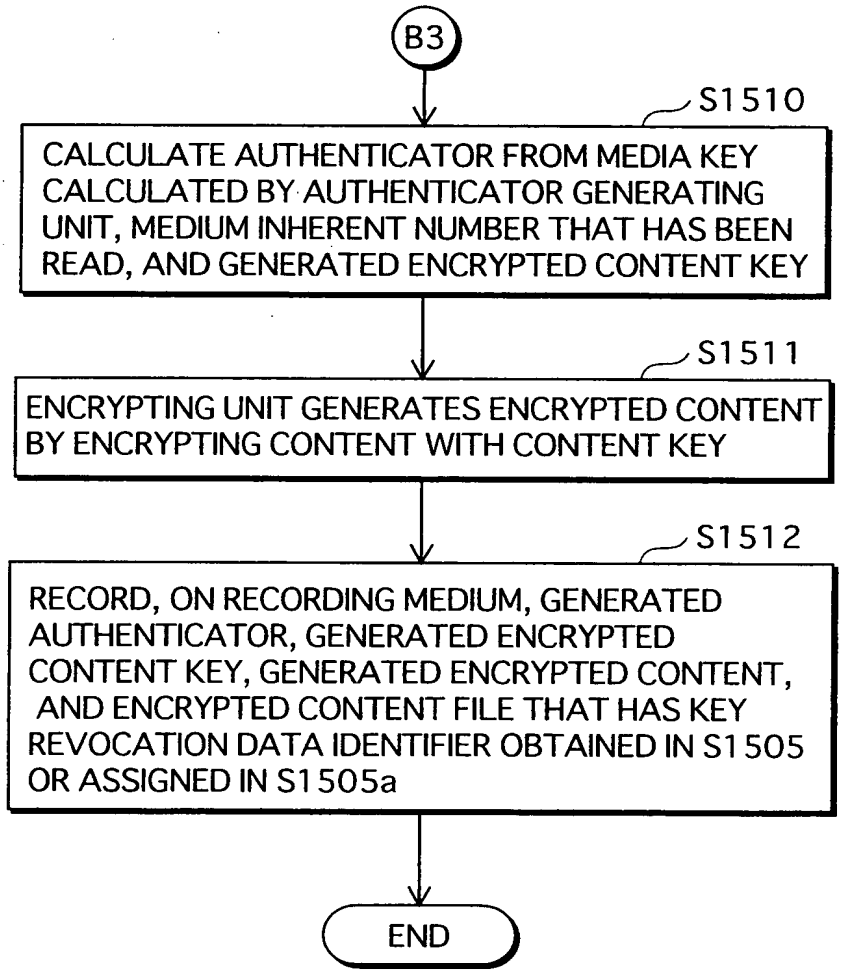

B3
S1510
CALCULATE AUTHENTICATOR FROM MEDIA KEY CALCULATED BY AUTHENTICATOR GENERATING UNIT, MEDIUM INHERENT NUMBER THAT HAS BEEN READ, AND GENERATED ENCRYPTED CONTENT KEY
S1511
ENCRYPTING UNIT GENERATES ENCRYPTED CONTENT BY ENCRYPTING CONTENT WITH CONTENT KEY
S1512
RECORD, ON RECORDING MEDIUM, GENERATED AUTHENTICATOR, GENERATED ENCRYPTED CONTENT KEY, GENERATED ENCRYPTED CONTENT, AND ENCRYPTED CONTENT FILE THAT HAS KEY REVOCATION DATA IDENTIFIER OBTAINED IN S1505 OR ASSIGNED IN S1505a
END

FIG.19

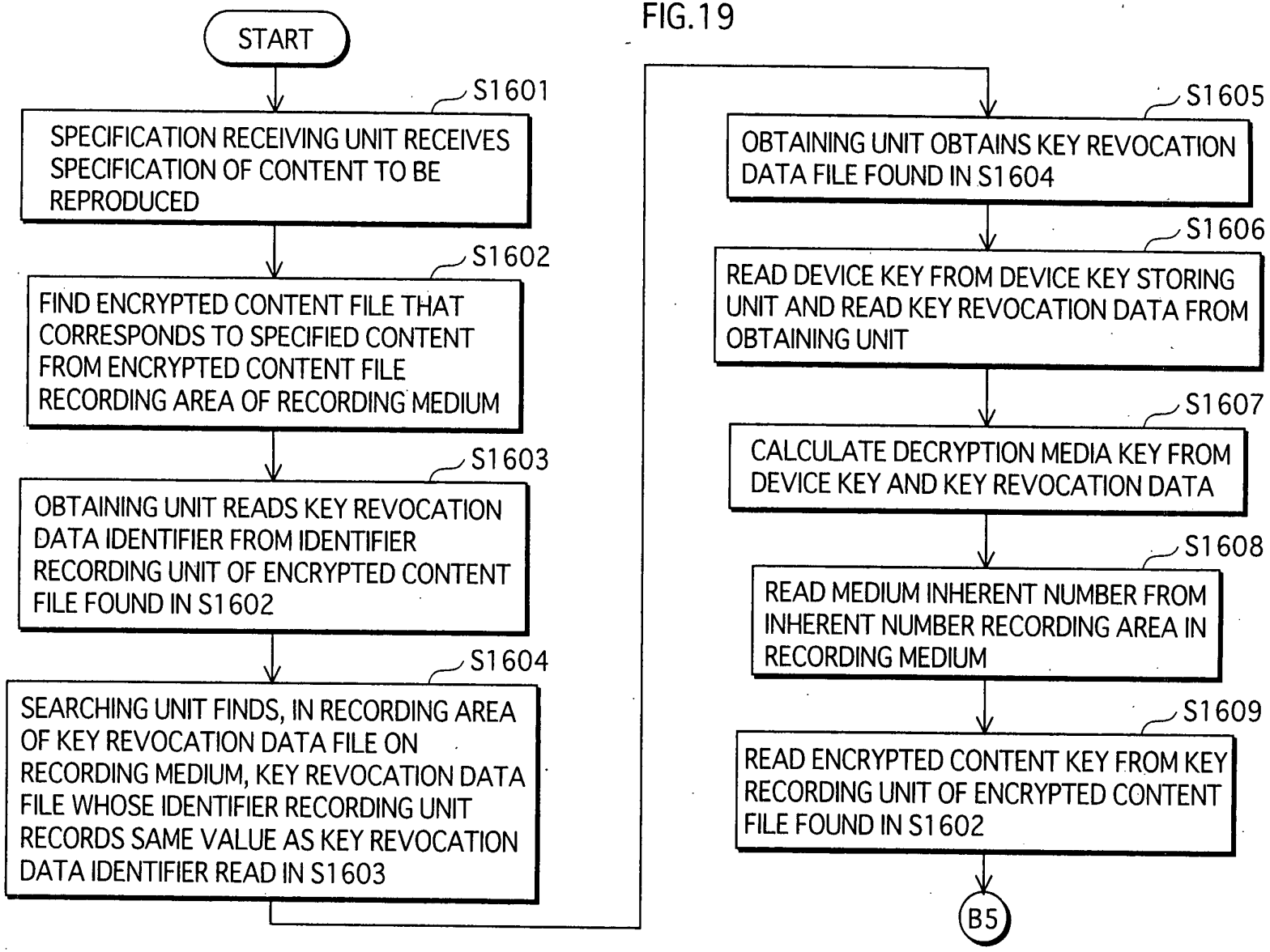
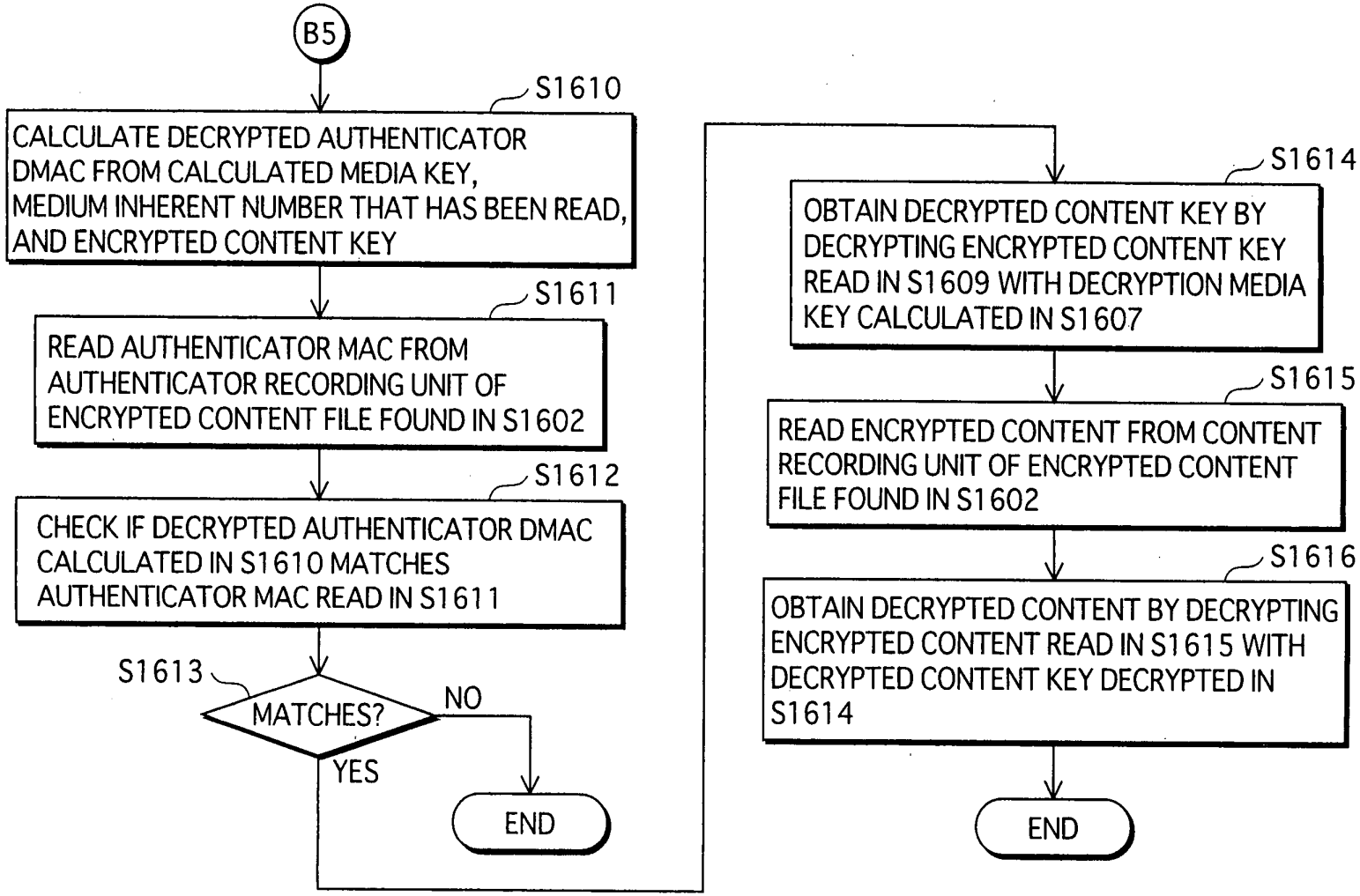

START
S1601
SPECIFICATION RECEIVING UNIT RECEIVES SPECIFICATION OF CONTENT TO BE REPRODUCED
S1602
FIND ENCRYPTED CONTENT FILE THAT CORRESPONDS TO SPECIFIED CONTENT FROM ENCRYPTED CONTENT FILE RECORDING AREA OF RECORDING MEDIUM
S1603
OBTAINING UNIT READS KEY REVOCATION DATA IDENTIFIER FROM IDENTIFIER RECORDING UNIT OF ENCRYPTED CONTENT FILE FOUND IN S1602
S1604
SEARCHING UNIT FINDS, IN RECORDING AREA OF KEY REVOCATION DATA FILE ON RECORDING MEDIUM, KEY REVOCATION DATA FILE WHOSE IDENTIFIER RECORDING UNIT RECORDS SAME VALUE AS KEY REVOCATION DATA IDENTIFIER READ IN S1603
S1605
OBTAINING UNIT OBTAINS KEY REVOCATION DATA FILE FOUND IN S1604
S1606
READ DEVICE KEY FROM DEVICE KEY STORING UNIT AND READ KEY REVOCATION DATA FROM OBTAINING UNIT
S1607
CALCULATE DECRYPTION MEDIA KEY FROM DEVICE KEY AND KEY REVOCATION DATA
S1608
READ MEDIUM INHERENT NUMBER FROM INHERENT NUMBER RECORDING AREA IN RECORDING MEDIUM
S1609
READ ENCRYPTED CONTENT KEY FROM KEY RECORDING UNIT OF ENCRYPTED CONTENT FILE FOUND IN S1602
B5

FIG.20


B5
S1610
CALCULATE DECRYPTED AUTHENTICATOR DMAC FROM CALCULATED MEDIA KEY, MEDIUM INHERENT NUMBER THAT HAS BEEN READ, AND ENCRYPTED CONTENT KEY
S1611
READ AUTHENTICATOR MAC FROM AUTHENTICATOR RECORDING UNIT OF ENCRYPTED CONTENT FILE FOUND IN S1602
S1612
CHECK IF DECRYPTED AUTHENTICATOR DMAC CALCULATED IN S1610 MATCHES AUTHENTICATOR MAC READ IN S1611
S1613
MATCHES?
NO
YES
END
S1614
OBTAIN DECRYPTED CONTENT KEY BY DECRYPTING ENCRYPTED CONTENT KEY READ IN S1609 WITH DECRYPTION MEDIA KEY CALCULATED IN S1607
S1615
READ ENCRYPTED CONTENT FROM CONTENT RECORDING UNIT OF ENCRYPTED CONTENT FILE FOUND IN S1602
S1616
OBTAIN DECRYPTED CONTENT BY DECRYPTING ENCRYPTED CONTENT READ IN S1615 WITH DECRYPTED CONTENT KEY DECRYPTED IN S1614
END